kernel, intrusion
Terms used: **kernel intrusion**

Found **642** of **251,056**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Open results in a new window

Refine these results with Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 642 Result page: 1 2 3 4 5 6 7 8 9 10 next >>

1 Kernel Based Intrusion Detection System

Byung-joo Kim, Il-kon Kim

July 2005 ICIS '05: Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05) - Volume 00, Volume 00

Publisher: IEEE Computer Society

Full text available: Publisher Site

Additional Information: full citation, abstract, index terms

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0

Recently applying artificial intelligence, machine learning and data mining techniques to intrusion detection system are increasing. But most of researches are focused on improving the performance of classifier. Selecting important features from input ...

2 A novel approach for a file-system integrity monitor tool of Xen virtual machine

Nguyen Anh Quynh, Yoshiyasu Takefuji
March 2007 ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security
Publisher: ACM
Full text available: pdf(253.86 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 37, Downloads (12 Months): 315, Citation Count: 0

File-system integrity tools (FIT) are commonly deployed host-based intrusion detections (HIDS) tool to detect unauthorized file-system changes. While FIT are widely used, this kind of HIDS has many drawbacks: the intrusion detection is not done in real-time ...

Keywords: Linux, Xen virtual machine, intrusion detection, rootkit

3 Towards a tamper-resistant kernel rootkit detector

Nguyen Anh Quynh, Yoshiyasu Takefuji
March 2007 SAC '07: Proceedings of the 2007 ACM symposium on Applied computing
Publisher: ACM
Full text available: pdf(177.12 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 28, Downloads (12 Months): 335, Citation Count: 0

A variety of tools and architectures have been developed to detect security violations to Operating System kernels. However, they all have fundamental flaw in the design so that they fail to discover kernel-level attack. Few hardware solutions have been ...

Keywords: Linux, Xen virtual machine, intrusion detection, kernel rootkit

4 BlueBoX: A policy-driven, host-based intrusion detection system

Suresh N. Chari, Pau-Chen Cheng
May 2003 ACM Transactions on Information and System Security (TISSEC), Volume 6 Issue 2
Publisher: ACM
Full text available: pdf(385.64 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 33, Downloads (12 Months): 226, Citation Count: 2

Detecting attacks against systems has, in practice, largely been delegated to sensors, such as network intrustion detection systems. However, due to the inherent limitations of these systems and the increasing use of encryption in communication, intrusion ...

Keywords: Intrusion detection, policy, sandboxing, system call introspection

5 Detecting worm variants using machine learning

Oliver Sharma, Mark Girolami, Joseph Sventek
December 2007 CoNEXT '07: Proceedings of the 2007 ACM CoNEXT conference
Publisher: ACM

Full text available: pdf(421.68 KB) Additional Information: full citation, abstract, references

Bibliometrics: Downloads (6 Weeks): 28, Downloads (12 Months): 38, Citation Count: 0

Network intrusion detection systems typically detect worms by examining packet or flow logs for known signatures. Not only does this approach mean worms cannot be detected until the signatures are created, but that variants of known worms will remain ...

6 Linear-Time Computation of Similarity Measures for Sequential Data

Konrad Rieck, Pavel Laskov
June 2008 The Journal of Machine Learning Research, Volume 9
Publisher: MIT Press

Full text available: pdf(570.38 KB) Additional Information: full citation, abstract

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 0, Citation Count: 0

Efficient and expressive comparison of sequences is an essential procedure for learning with sequential data. In this article we propose a generic framework for computation of similarity measures for sequences, covering various kernel, distance and non-metric ...

7 Masquerade detection based on SVM and sequence-based user commands profile

Jeongseok Seo, Sungdeok Cha
March 2007 ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security
Publisher: ACM

Full text available: pdf(149.25 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 16, Downloads (12 Months): 143, Citation Count: 0

Masqueraders, despite widespread use of security products such as firewalls and intrusion detection systems, are serious threats to organizations. Although anomaly detection techniques have been considered as an effective approach to complement existing ...

Keywords: anomaly detection, masquerade detection, support vector machine (SVM), user commands profile

8 Scanning workstation memory for malicious codes using dedicated coprocessors

Sirish A. Kondi, Yoginder S. Dandass

March 2006 ACM-SE 44: Proceedings of the 44th annual Southeast regional conference

Publisher: ACM

Full text available: pdf(176.91 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 2, Downloads (12 Months): 69, Citation Count: 0

This paper describes the implementation of a coprocessor platform for scanning workstation memory in order to detect signatures of malicious codes. The coprocessor is especially beneficial in clusters of workstations used for high performance computing ...

Keywords: FPGA, coprocessor, intrusion detection, signature matching

9 Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation

Georgios Portokalidis, Asia Slowinska, Herbert Bos

October 2006 ACM SIGOPS Operating Systems Review, Volume 40 Issue 4

Publisher: ACM

Full text available: pdf(471.94 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 20, Downloads (12 Months): 164, Citation Count: 5

As modern operating systems and software become larger and more complex, they are more likely to contain bugs, which may allow attackers to gain illegitimate access. A fast and reliable mechanism to discern and generate vaccines for such attacks is vital ...

10 Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation

Georgios Portokalidis, Asia Slowinska, Herbert Bos

April 2006 EuroSys '06: Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems 2006

Publisher: ACM

Full text available: pdf(471.94 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 20, Downloads (12 Months): 164, Citation Count: 5

As modern operating systems and software become larger and more complex, they are more likely to contain bugs, which may allow attackers to gain illegitimate access. A fast and reliable mechanism to discern and generate vaccines for such attacks is vital ...

11 Self-healing mechanisms for kernel system compromises

Sandra Ring, David Esler, Eric Cole

October 2004 WOSS '04: Proceedings of the 1st ACM SIGSOFT workshop on Self-managed systems

Publisher: ACM

Full text available: pdf(78.66 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 92, Citation Count: 0

Increasing demands for reliability and dependability clash with the reality of escalating security compromises and vulnerability discoveries. Improvements in attack methodologies such as polymorphic viruses, tampering of source code repositories, and ...

Keywords: fault tolerance, kernel, operating systems, self-healing systems

12 Applications of a feather-weight virtual machine

Yang Yu, Hariharan Kolam, Lap-Chung Lam, Tzi-cker Chiueh

March 2008 VEE '08: Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments

Publisher: ACM

Full text available: pdf(302.75 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 51, Downloads (12 Months): 217, Citation Count: 0

A Feather-weight Virtual Machine (FVM) is an OS-level virtualization technology that enables multiple isolated execution environments to exist on a single Windows kernel. The key design goal of FVM is efficient resource sharing among VMs so as to minimize ...

Keywords: binary server, browser exploit, information theft, virtual machine, web crawler

13 Exact multi-pattern string matching on the cell/b.e. processor

Daniele Paolo Scarpazza, Oreste Villa, Fabrizio Petrini
May 2008 CF '08: Proceedings of the 2008 conference on Computing frontiers
Publisher: ACM
Full text available: pdf(586.74 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 34, Downloads (12 Months): 34, Citation Count: 0

String searching is the computationally intensive kernel of many security and network applications like search engines, intrusion detection systems, virus scanners and spam filters. The growing size of on-line content and the increasing wire speeds push ...

Keywords: cell processor, matching, string

14 Catching spam before it arrives: domain specific dynamic blacklists

Duncan Cook, Jacky Hartnett, Kevin Manderson, Joel Scanlan
January 2006 ACSW Frontiers '06: Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54, Volume 54
Publisher: Australian Computer Society, Inc.
Full text available: pdf(160.06 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 26, Downloads (12 Months): 276, Citation Count: 1

The arrival of any piece of unsolicited and unwanted email (spam) into a user's email inbox is a problem. It results in real costs to organisations and possibly an increasing reluctance to use email by some users. Currently most spam prevention techniques ...

15 Core Vector Machines: Fast SVM Training on Very Large Data Sets

Ivor W. Tsang, James T. Kwok, Pak-Ming Cheung
December 2005 The Journal of Machine Learning Research, Volume 6
Publisher: MIT Press
Additional Information: full citation, abstract, cited by

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 11

Standard SVM training has $O(m^3)$ time and $O(m^2)$ space complexities, where m is the training set size. It is thus computationally infeasible on very large data sets. By observing that practical SVM ...

16 The taser intrusion recovery system

Ashvin Goel, Kenneth Po, Kamran Farhadi, Zheng Li, Eyal de Lara
October 2005 ACM SIGOPS Operating Systems Review, Volume 39 Issue 5
Publisher: ACM

Full text available: pdf(346.32 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 140, Citation Count: 0

Recovery from intrusions is typically a very time-consuming operation in current systems. At a time when the cost of human resources dominates the cost of computing resources, we argue that next generation systems should be built with automated intrusion ...

Keywords: file systems, intrusion analysis, intrusion recovery, snapshots

17 The taser intrusion recovery system

Ashvin Goel, Kenneth Po, Kamran Farhadi, Zheng Li, Eyal de Lara
October 2005 SOSP '05: Proceedings of the twentieth ACM symposium on Operating systems principles
Publisher: ACM

Full text available: pdf(346.32 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 15, Downloads (12 Months): 140, Citation Count: 0

Recovery from intrusions is typically a very time-consuming operation in current systems. At a time when the cost of human resources dominates the cost of computing resources, we argue that next generation systems should be built with automated intrusion ...

Keywords: file systems, intrusion analysis, intrusion recovery, snapshots

18 Proceedings of the 2005 conference on Genetic and evolutionary computation

Una-May O'Reilly, Hans-Georg Beyer
June 2005 proceeding
Publisher: ACM

Additional Information: full citation, appendices and supplements, abstract

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 1

The papers in this two volume proceedings are presented at the 7th Annual Genetic and Evolutionary Computation COnference (GECCO-2005), held in Washington, D.C., June 25-29, 2005.This year is an exceptional one for the GECCO conference series. First, ...

19 Proceedings of the 9th annual conference on Genetic and evolutionary computation

Hod Lipson
July 2007 proceeding
Publisher: ACM
Additional Information: full citation, appendices and supplements, abstract

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0

These proceedings contain the papers presented at the *9th Annual Genetic and Evolutionary Computation COnference* (GECCO-2007), held in London, UK, July 7-11, 2007. For the first time GECCO was held outside the US. This clearly proved ...

20 Backtracking intrusions

Samuel T. King, Peter M. Chen
February 2005 ACM Transactions on Computer Systems (TOCS), Volume 23 Issue 1
Publisher: ACM
Full text available: pdf(647.38 KB) Additional Information: full citation, abstract, references, cited by, index terms, review

Bibliometrics: Downloads (6 Weeks): 31, Downloads (12 Months): 199, Citation Count: 2

Analyzing intrusions today is an arduous, largely manual task because system administrators lack the information and tools needed to understand easily the sequence of steps that occurred in an attack. The goal of BackTracker is to identify automatically ...

Keywords: Computer forensics, information flow, intrusion analysis

PORTAL USPTO

Advanced Search

THE ACM DIGITAL LIBRARY

No results were found.

Please revise or start a new search instead

Enter words, phrases or names below to revise your search.
Surround phrases or full names with double quotation marks.

Edit the query directly, or use the form below

"kernel audit record", intrusion

Search

Words or Phrases

Find [any field] with

all of this text (and)

any of this text (or)

none of this text (not)

Names

Find [any field] with names

using all any none of the names

Keywords

Find author's keywords

using all any none of the keywords

Affiliations

Find company or school

using all any none of the affiliations

Publication

Find publication

using all any none of the names

Find publisher

using any none of the names

Published since [year]

Published before [year]

In publication types: Journal Proceeding Transaction Magazine Newsletter

Conference

Find sponsor names

using all any none of the names

Find location

using any none of the locations

Find year (yyyy)

using any none of the years

Identification codes

Find ISBN/ ISSN

Find DOI

Computing Classification System (CCS)

Find node

Find subject/ noun

☐ Look at primary category only

Required components

Results must have ☐ Full Text ☐ Abstract ☐ Review